PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-164548
(43)Date of publication of application : 19.06.1998

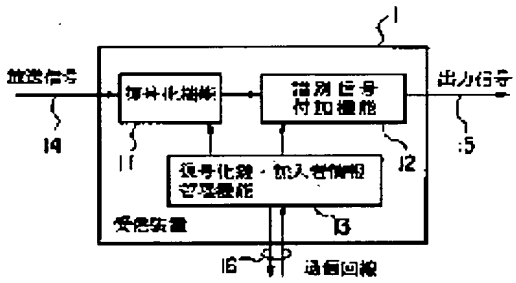
(51)Int.Cl. H04N 7/167

(21)Application number : 08-313641
(22)Date of filing : 25.11.1996

(71)Applicant : TOSHIBA CORP
(72)Inventor : HASHIMOTO MIKIO
TAKAHATA YOSHIAKI

(54) RECEIVER, BROADCASTING SYSTEM AND RECEPTION METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To prevent duplication of a work object from being illegally distributed and sold and to specify the source, even when a broadcasted work object is duplicated and distributed by adding a signal for specifying a subscriber (receiver) to the signals outputted from a present device in a receiver installed on a subscriber side.
SOLUTION: For this receiver 1, the one for which broadcasting is ciphered is defined as an object, so as to inhibit the interception of the broadcasting of a non-subscriber and only the receiver 1 of the subscriber for which the decoding key of cipher is registered can obtain it. Ciphered broadcasting signals are inputted from an input line 14 and deciphered in a deciphering part 11. Identification signals, including identification information for specifying the subscriber, are added to the deciphered signals in an identification signal addition part 12 and they are outputted from an output line 15. A key used for deciphering and information added as the identification signals are obtained from a broadcasting management system on a broadcasting station side through a communication channel 16 by a deciphering key/subscriber information management part 13.



LEGAL STATUS

[Date of request for examination] 06.09.2000
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（A）**　(11)特許出願公開番号

特開平10－164548

(43)公開日　平成10年(1998)６月19日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｈ０４Ｎ　7/167		Ｈ０４Ｎ　7/167	Ｚ

審査請求　未請求　請求項の数８　ＯＬ　（全 11 頁）

(21)出願番号　特願平8－313641

(22)出願日　平成８年(1996)11月25日

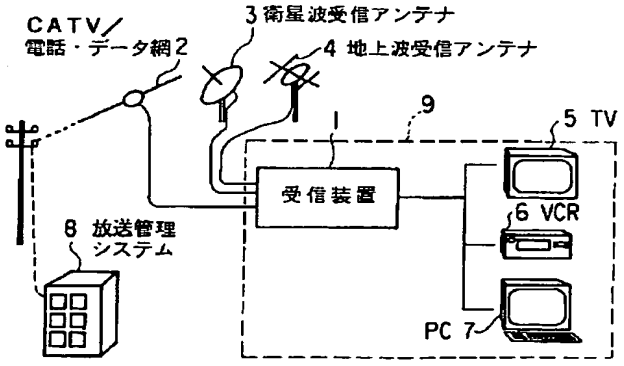
(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地
(72)発明者　橋本　幹生
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内
(72)発明者　高畠　由彰
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内
(74)代理人　弁理士　鈴江　武彦　（外６名）

(54)【発明の名称】　受信装置、放送システム及び受信方法

(57)【要約】

【課題】　限定された複数の加入者に放送される放送信号が受信され媒体に複製された場合に、該放送信号の複製主体を特定できるようにした受信装置を提供すること。

【解決手段】　登録された加入者を対象として放送される放送信号を受信するために加入者側に設置される受信装置において、受信した前記放送信号に、少なくとも該放送信号を受信した前記加入者を特定する情報を含む付加信号を付加する手段を備えたことを特徴とする。また、前記放送局側から放送される放送信号には、該放送局を特定する放送局識別信号が付加されており、前記付加信号を付加する手段は、前記放送局識別信号の信号付加形式をもとにして、予め定められた複数の信号付加形式のうちから、前記付加信号の付加に用いる信号付加形式を選択するようにする。



1

【特許請求の範囲】

【請求項１】登録された加入者を対象として放送される放送信号を受信するために加入者側に設置される受信装置において、

受信した前記放送信号に、少なくとも該放送信号を受信した前記加入者を特定する情報を含む付加信号を付加する手段を備えたことを特徴とする受信装置。

【請求項２】登録された加入者を対象とするために内容を暗号化して放送された放送信号を受信し復号する、加入者との対応が放送局側により管理された受信装置において、

受信し復号された前記放送信号に、少なくとも該放送信号を受信した該受信装置に対応する前記加入者を特定する情報を含む付加信号を付加する手段を備えたことを特徴とする受信装置。

【請求項３】前記放送局側から放送される放送信号には、該放送局を特定する情報を含む放送局識別信号が付加されており、

前記付加信号を付加する手段は、前記放送局識別信号の信号付加形式をもとにして、予め定められた複数の信号付加形式のうちから、前記付加信号の付加に用いる信号付加形式を選択することを特徴とする請求項１または２に記載の受信装置。

【請求項４】前記付加信号の信号付加方式は、特定の符号語を用いた時間領域または空間領域のスペクトル拡散方式によるものであり、

前記付加信号を付加する手段は、前記付加信号の付加に用いる符号語として、前記放送局識別信号と前記付加信号に使用する符号語が互いに直交する符号語となるものを選択することを特徴とする請求項３に記載の受信装置。

【請求項５】自装置を他の装置から識別可能な装置識別情報が記憶された識別情報記憶部と、

第３者が外部から自装置にアクセスして、前記識別情報記憶部に記憶された前記装置識別情報を取得することを不能にする手段と、

前記放送信号を放送する放送局側との間で自装置の正当性の認証を行うために、前記識別情報記憶部に記憶された装置識別情報をもとにして生成された所定の認証情報を自装置外部に送信するときに、第３者がこの送信された所定の認証情報を傍受して前記装置識別情報を取得することを不能にする手段と、

第３者が外部から自装置にアクセスして、自装置が受信した前記放送信号であって前記付加信号がまだ付加されていない状態のものを取得することを不能にする手段とを備えたことを特徴とする請求項１ないし４のいずれか１項に記載の受信装置。

【請求項６】登録された加入者を対象とするために内容を暗号化して放送信号を放送する放送局側の送信システムと、放送局側が各加入者の情報を管理する放送管理システムと、各加入者側に設置されて該放送信号を受信し復号する受信装置とを備えた放送システムにおいて、

前記放送管理システムは、加入者を特定する情報と、該加入者側に設置された前記受信装置を特定する情報との対応を管理する手段と、

各受信装置との間で受信装置の認証を行う手段と、

この認証によって正当と判断された受信装置に、前記放送信号を復号するために用いる復号鍵を指定する第１の指定情報と、該受信装置側で受信された該放送信号に付加する信号に含めるべき、少なくとも該放送信号を受信した該受信装置に対応する前記加入者を特定する情報を含む識別情報を指定する第２の指定情報とを送信する手段とを備え、

前記受信装置は、前記放送管理システムに対し自装置の認証を行う手段と、

この認証に通った場合に、前記放送管理システムから送信される、第１の指定情報と、第２の指定情報とを受信する手段と、

自装置が受信し、前記第１の指定情報により指定される復号鍵を用いて復号された前記放送信号に、第２の指定情報により指定される識別情報を含む付加信号を付加する手段を備えたことを特徴とする放送システム。

【請求項７】登録された加入者を対象として放送される放送信号を受信するために加入者側に設置される受信装置の受信方法において、

受信された前記放送信号に、少なくとも該放送信号を受信した前記加入者を特定する情報を含む付加信号を付加することを特徴とする受信方法。

【請求項８】登録された加入者を対象とするために内容を暗号化して放送された放送信号を受信し復号する、加入者との対応が放送局側により管理された受信装置の受信方法において、

受信され復号された前記放送信号に、少なくとも該放送信号を受信した該受信装置に対応する前記加入者を特定する情報を含む付加信号を付加することを特徴とする受信方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、複数の相手に同一内容の著作物を配布する放送システム、この放送システムにおける受信装置および受信方法に関する。

【０００２】

【従来の技術】家庭、エンドユーザに向けた通信、放送のデジタル化が進められている。これによって、従来のテレビやラジオも多様な情報が提供可能になり、またビデオオンデマンド（ＶＯＤ）のような新しいサービスも可能になりつつある。

【０００３】一方、映像、音声メディアのデジタル化によって劣化の少ない著作物のコピーが可能になりつつある。これは，利用者には利益をもたらすが、著作物の製

作者にとっては複製による著作権の侵害の脅威となる。

【０００４】この問題を解決する従来の技術として、著作物に、それがある著作権者に属することを示す「サイン」を入れる方法がある。例えば放送される映画の画面に隅にその配給会社名もしくは放送する放送局名を入れておく方法である。しかしこの方法は、著作物の鑑賞の妨げになるばかりでなく、著作物の改変にあたると判断されるおそれもある。一方で、この方法では著作物を損なうことなくサインを取り除くことは困難なため、著作物保護の効果は高い。

【０００５】別な方法として、著作物に付加的な信号を与え、そこに著作権者に関する情報またはコピーの可／不可を記述する方法がある。音声メディアではＤＡＴやＭＤにおいて実現されている。この方式の問題は、付加的な信号は著作物を損なうことなく比較的簡単に除去が可能なことである。一度付加的な信号が除去されてしまえば原版とまったく同一の複製である海賊版が自由に出回ることになる。

【０００６】ここで、著作物の内容に利用者に見えない「透かし」（ｗａｔｅｒｍａｒｋ）の形で識別情報を不可することは著作物の鑑賞を妨げず、また複製を防止する手段として有効である（例えば、“Ｃｒｙｐｔｏｌｏｇｙ ｆｏｒ Ｄｉｇｉｔａｌ ＴＶ Ｂｒｏａｄｃａｓｔｉｎｇ”，Ｂｅｎｏｉｔ Ｍ．Ｍａｃｑ，ａｎｄ Ｊｅａｎ－Ｊａｃｑｕｅｓ Ｑｕｉｓｑｕａｔｅｒ，Ｐｒｏｃｅｅｄｉｎｇｓ ｏｆ ｔｈｅ ＩＥＥＥ，８３（６）：９４４，１９９５）。

【０００７】「透かし」の用途としては、著作物の権利者の表示あるいは権利者が設定されている場合のコピー禁止機能がある。テープあるいはディスクによる配布では、そのシリアル番号も含まれ、海賊版の複製元を特定することにも利用可能である。

【０００８】著作物にシリアル番号のような識別情報を付加しておけば、著作権者は大量の海賊版が出回った際にその複製元を特定し、法的手段を行使することによって被害を防ぐことができる。識別子の付加は利用者の私的コピーの権利を制限することなく著作者の権利を保護できる点が優れている。

【０００９】また、近年ソフトウェアにおいてシェアウェアという概念が広まっている。これは、ソフトウェア自体に利用の制限を設けないために誰もが自由に使えるが、一定の基準を越えた利用にはそれに相当する対価を支払うというものである。この概念はより広い一般の著作物にも適用でき、ある映画の一部を利用したビデオクリップを作成する場合、コピーが完全に禁止されていれば予め映画の著作者の許可を得なければならないが、私的コピーが自由ならば映画を引用してビデオクリップを作成した後、販売する段階で許可を得れば良い。これはマルチメディアコンテンツの流通を促進する効果がある。

【００１０】ところが、従来は放送やビデオオンデマンドにおいては同一の著作物が複数の利用者に配布されるため、それらへ利用者毎に別々の識別情報を付加することはできなかった。

【００１１】

【発明が解決しようとする課題】利用者の権利と著作権者の権利の両立の手段としてその著作物が誰に向けて利用権を与えられたものであるかを示す識別情報を付加することが有効である。とりわけ利用者に関知できず、取り除くことのできない「透かし」の形で付加することが著作権保護の観点からは望ましい。

【００１２】ところが、従来は放送系やビデオオンデマンドにおいては同一の著作物が複数のユーザに配布されるため、それらに別々の識別情報を付加することはできないという問題があった。また、付加する信号が悪意のユーザによって改変されてしまうことを防がなければならない。

【００１３】さらに、著作権保護は著作物複製流通の各段階で行われることが望ましい。そのためには複数回に分けて識別情報を付加することが必要になる。例えば、著作権者から放送局への複製の段階と、放送局からエンドユーザである利用者への複製の段階である。このように複数回にわたって付加される識別情報が読み取りにおける互いの識別性を損なったり、著作物の品質を低下させることも防がなければならない。

【００１４】本発明は、上記事情を考慮してなされたもので、限定された複数の加入者に放送される放送信号が受信され媒体に複製された場合に、該放送信号の複製主体を特定できるようにした受信装置、放送システム及び受信方法を提供することを目的とする。

【００１５】

【課題を解決するための手段】本発明（請求項１）は、登録された加入者を対象として放送される放送信号を受信するために加入者側に設置される受信装置において、受信した前記放送信号に、少なくとも該放送信号を受信した前記加入者を特定する情報を含む付加信号を付加する手段を備えたことを特徴とする。

【００１６】本発明によれば、放送系やビデオオンデマンドのように同一の著作物が複数のユーザに配布される、加入者を限定した放送システムにおいて、加入者側に設置される受信装置において、自装置から出力される信号に加入者（受信者）を特定する信号を付加するようにすることで、加入者毎に別々の識別情報を付加することができる。

【００１７】これによって、不法に著作物の複製が頒布・販売されるのを未然に防止するとともに、万一、放送された著作物が複製され流通されたとしても、その出所を特定することができる。

【００１８】本発明（請求項２）は、登録された加入者を対象とするために内容を暗号化して放送された放送信

号を受信し復号する、加入者との対応が放送局側により管理された受信装置において、受信し復号された前記放送信号に、少なくとも該放送信号を受信した該受信装置に対応する前記加入者を特定する情報を含む付加信号を付加する手段を備えたことを特徴とする。

【００１９】本発明によれば、放送系やビデオオンデマンドのように同一の著作物が複数のユーザに配布される、加入者を限定した放送システムにおいて、加入者側に設置される受信装置において、自装置から出力される信号に加入者（受信者）を特定する信号を付加するようにすることで、加入者毎に別々の識別情報を付加することができる。

【００２０】これによって、加入者以外の第３者に著作物を取得されて、識別情報が付加されていない著作物の不正な複製が流通することを防ぐことができる。本発明（請求項３）は、請求項１または２に記載の受信装置において、前記放送局側から放送される放送信号には、該放送局を特定する情報を含む放送局識別信号が付加されており、前記付加信号を付加する手段は、前記放送局識別信号の信号付加形式をもとにして、予め定められた複数の信号付加形式のうちから、前記付加信号の付加に用いる信号付加形式を選択することを特徴とする。

【００２１】本発明によれば、複数回にわたって付加される、著作物の受け渡しにかかわった主体（放送局と加入者）を特定する情報を含む信号が、互いに干渉してその読み取りにおける互いの識別性を損なうことと、著作物の品質を低下させることを防ぐことができる。

【００２２】本発明（請求項４）は、請求項３に記載の受信装置において、記付加信号の信号付加方式は、特定の符号語を用いた時間領域または空間領域のスペクトル拡散方式によるものであり、前記付加信号を付加する手段は、前記付加信号の付加に用いる符号語として、前記放送局識別信号と前記付加信号に使用する符号語が互いに直交する符号語となるものを選択することを特徴とする。

【００２３】本発明によれば、放送信号に付加されている放送局識別信号の形式をもとに受信装置において付加される付加信号に適切な形式を選択することにより、付加された各信号に含まれる情報の読み取りにおける互いの識別性を損なったり、著作物の品質を低下させることを防止することができる。

【００２４】本発明（請求項５）は、請求項１ないし４のいずれか１項に記載の受信装置において、自装置を他の装置から識別可能な装置識別情報が記憶された識別情報記憶部と、第３者が外部から自装置にアクセスして、前記識別情報記憶部に記憶された前記装置識別情報を取得することを不能にする手段と、前記放送信号を放送する放送局側との間で自装置の正当性の認証を行うために、前記識別情報記憶部に記憶された装置識別情報をもとにして生成された所定の認証情報を自装置外部に送信するときに、第３者がこの送信された所定の認証情報を傍受して前記装置識別情報を取得することを不能にする手段と、第３者が外部から自装置にアクセスして、自装置が受信した前記放送信号であって前記付加信号がまだ付加されていない状態のものを取得することを不能にする手段とを備えたことを特徴とする。

【００２５】ここで、第３者が外部から自装置にアクセスして、前記識別情報記憶部に記憶された前記装置識別情報を取得することを不能にする手段と第３者が外部から自装置にアクセスして、自装置が受信した前記放送信号であって前記付加信号がまだ付加されていない状態のものを取得することを不能にする手段は、例えば、耐タンパーな性質を持つ装置筐体を用いることで実現可能である。

【００２６】また、前記放送信号を放送する放送局側との間で自装置の正当性の認証を行うために、前記識別情報記憶部に記憶された装置識別情報をもとにして生成された所定の認証情報を自装置外部に送信するときに、第３者がこの送信された所定の認証情報を傍受して前記装置識別情報を取得することを不能にする手段は、例えば、受信装置が放送局側に正当な装置識別子を持つことを証明する手続きにゼロ知識証明方式を用いることで実現可能である。

【００２７】本発明によれば、加入者側の受信装置に不正を働くことによってあるいは不正な受信装置を使うことによって、識別情報が付加されない著作物の不正な流通を防ぐことができる。

【００２８】本発明（請求項６）は、登録された加入者を対象とするために内容を暗号化して放送信号を放送する放送局側の送信システムと、放送局側が各加入者の情報を管理する放送管理システムと、各加入者側に設置されて該放送信号を受信し復号する受信装置とを備えた放送システムにおいて、前記放送管理システムは、加入者を特定する情報と、該加入者側に設置された前記受信装置を特定する情報との対応を管理する手段と、各受信装置との間で受信装置の認証を行う手段と、この認証によって正当と判断された受信装置に、前記放送信号を復号するために用いる復号鍵を指定する第１の指定情報と、該受信装置側で受信された該放送信号に付加する信号に含めるべき、少なくとも該放送信号を受信した該受信装置に対応する前記加入者を特定する情報を含む識別情報を指定する第２の指定情報とを送信する手段とを備え、前記受信装置は、前記放送管理システムに対し自装置の認証を行う手段と、この認証に通った場合に、前記放送管理システムから送信される、第１の指定情報と、第２の指定情報とを受信する手段と、自装置が受信し、前記第１の指定情報により指定される復号鍵を用いて復号された前記放送信号に、第２の指定情報により指定される識別情報を含む付加信号を付加する手段を備えたことを特徴とする。

【００２９】また、本発明（請求項７）は、登録された加入者を対象として放送される放送信号を受信するために加入者側に設置される受信装置の受信方法において、受信された前記放送信号に、少なくとも該放送信号を受信した前記加入者を特定する情報を含む付加信号を付加することを特徴とする。

【００３０】本発明（請求項８）は、登録された加入者を対象とするために内容を暗号化して放送された放送信号を受信し復号する、加入者との対応が放送局側により管理された受信装置の受信方法において、受信され復号された前記放送信号に、少なくとも該放送信号を受信した該受信装置に対応する前記加入者を特定する情報を含む付加信号を付加することを特徴とする。なお、各装置に係る発明は、方法に係る説明としても成立する。

【００３１】

【発明の実施の形態】以下、図面を参照しながら発明の実施の形態を説明する。図１に、本発明の一実施形態に係る放送・受信システムの構成の一例を示す。図中、９は加入者宅内のシステムである。また、２はＣＡＴＶあるいは電話／データ通信網への接続を、３は衛星放送受信アンテナを、４は地上波放送受信アンテナをそれぞれ示す。

【００３２】放送管理システム８は、各放送局ごとに（または所定数もしくは全ての放送局について１つ）設置され、各加入者宅の受信装置１との間で、当該受信装置１の装置認証、復号鍵の配送、課金情報の収集、その他必要な情報のやりとりを行う。

【００３３】本実施形態では、各加入者宅内に設置される受信装置１にはそれぞれ、その装置を特定可能な装置識別子が付与されるものとする。また、各加入者には、それぞれを特定可能な加入者番号などの加入者識別情報が割り当てられるものとする。加入者の識別情報と、該加入者宅内に設置された受信装置１の装置識別子との対応は、放送管理システム８にて管理されているものとする。

【００３４】加入者宅に設置された受信装置１は、少なくとも１つの放送入力を持つ。放送入力は、例えば地上波放送（ＶＨＦ／ＵＨＦ）、衛生放送、ケーブルＴＶ、通信網による放送のいずれでも良い。図１においては１つの受信装置１で複数の放送入力に対応する例を示しているが、放送形式の数や組み合わせは任意である。もちろん、任意の１つの放送形式の入力を持つものも存在し得る。

【００３５】また、受信装置１は、放送入力に加えて放送管理システム８との双方向の通信が可能な通信手段を持つ。この通信手段は、放送の伝送媒体にケーブルＴＶを用いる場合には、コスト低減のためにケーブルＴＶ自身が持つ放送局側システムとの双方向通信機能を用いることが望ましい。この場合、ケーブルは放送波の伝送と共用されることになる。一方、衛星放送や地上波の場合にはこの通信手段として、放送の伝送媒体とは別のもの、例えば電話網を用いても良い。この通信手段は、受信装置の認証、課金と暗号化された放送内容の復号に用いる鍵を配送するためなどに用いられる。

【００３６】受信装置１は、ＣＡＴＶ、衛星放送あるいは地上波放送などの放送局から放送されネットワークを介してあるいはアンテナから受信された暗号化された信号（あるいは圧縮処理され暗号化された信号）を、復号化し（あるいは復号化し伸張処理し）、さらに加入者（受信者）を特定可能な情報が含まれている識別信号を付加して、ＴＶ５、ＶＴＲ６あるいはパーソナルコンピュータ（ＰＣ）７などの加入者の再生装置に出力する。

【００３７】加入者を特定可能な情報としては、まず加入者識別情報を用いることが考えられる。加入者識別情報と受信装置１の装置識別子が１対１に対応している場合には、装置識別子を用いても良い。また、加入者識別情報と受信装置１の装置識別子の両方を用いても良い。

【００３８】受信装置１の出力は、既存のＴＶ用ケーブルを利用したＶＨＦ帯の変調信号、あるいはＮＴＳＣビデオ、また、デジタル化されたＴＶやＶＣＲのインタフェース（ＩＥＥＥ　１９３４：“ＩＥＥＥ　Ｐ１３９４　Ｓｔａｎｄａｒｄ　ｆｏｒＨｉｇｈ　Ｐｅｒｆｏｒｍａｎｃｅ　Ｓｅｒｉａｌ　Ｂｕｓ　Ｄｒａｆｔ　８．３ｖ１”，ＩＥＥＥ，１９９６）等のいずれか、またはそれらの組合せであっても良い。

【００３９】ここで、本実施形態における放送局や放送管理システムは、無線電波やケーブルＴＶのような特定の伝送方式と番組制作・提供を目的とした形態に限らず、同一の著作物を複数の利用者に配布するサービス全般におけるものを含むものである。例えば、伝送手段が１種類に限定されないインターネット上の放送サービスや、定められたスケジュールに従って放送を行う番組としての形態をとらずに利用者からの要求に応答してサービスが行われる相互作用的な画像検索・提供サービスを含むものである。

【００４０】図２に、本実施形態に係る受信装置１の基本構成を示す。概略的には、この受信装置１は、非加入者の放送の傍受を禁止するために放送が暗号化されているものを対象とし、暗号の復号鍵を正当な加入者（登録された加入者）の受信装置１のみが入手できるようにするための通信機能を持ち、そして、受信した放送信号を復号化し、これに識別信号を付加して出力する機能を持つものである。

【００４１】図２において、入力ライン１４から暗号化された放送信号が入力され、復号化部１１で復号化される。復号化された信号に識別信号付加部１２で、加入者を特定する識別情報を含む識別信号が付加され、出力ライン１５から出力される。復号化に用いられる鍵や、識別信号として付加される情報は、復号化鍵・加入者情報管理部１３が通信回線１６を通して放送局側の放送管理

システム８から入手する。既に説明したように入力ライン１４と通信回線１６は物理的に同一の伝送媒体であっても構わない。

【００４２】識別信号には、例えば、加入者の識別番号、受信装置１の装置識別子、放送内容のタイトル、放送時刻などの付加的な情報が含まれる。この識別信号は、原信号の質を損なうことなく取り去ることができない形で付加するものとする。これは、例えば、「“Cryptology for Digital TV Broadcasting”, Benoit M. Macq, and Jean－Jacques Quisquater, Proceedings of the IEEE, 83 (6) : 944, 1995」や「“Digital Watermarks for Audio Signals”, L. Bonuey 他, Proceedings of International Conference on multimedia computing and systems, IEE, 1996」に開示された技術を用いることにより実現可能である。

【００４３】このため、仮に放送された番組が複製され流通されたとしても、それがいつ、誰に配布したものであるかが識別信号を検査することによってわかり、著作権および放送局は関連する法律に基づいて適切な処置を取ることができる。

【００４４】ただし、悪意の第３者が、ある加入者の利用している放送内容を盗みとった上で複製して販売した場合には、コンテンツ複製の疑いは正当な加入者にかかるとになる。

【００４５】これを防ぐために受信装置１から再生・記憶装置までの伝送手段には悪意の第３者によるアクセスを防ぐ手段が講じられていることが望ましい。本実施形態では、前記伝送手段の利用は家庭の中における番組の配送に限定される。従って一般に家庭内には悪意の第３者が侵入し難いので、例えば伝送手段に光ファイバーを用いるなどして不要な放射が生じないようにすれば良い。

【００４６】また、受信装置１の中には暗号化されていた放送信号が復号化部１１によって復号化された状態で存在する。放送局側の立場から見れば悪意の加入者によって識別信号が付加されていない原信号を読み出され、複製されてしまう危険がある。識別信号が付加されていない原信号が上述のように複製を禁止することができないためである。従って、受信装置外部からの信号の読み出しを禁止する手段を講じることが望ましい。

【００４７】このような装置への不正なアクセスや破壊的手段による内部情報の読み出しを禁止する手段は、耐タンパーな装置として既に知られている技術を用いることにより実現可能である（例えば、Mori, R., Kawahara, M: “Superdistribution: The Concept and theArchitecture”, IEICE transaction 73 (7), 1990）。

【００４８】前述の耐タンパー性に加えて、加入者側の受信装置１は自装置が前述の耐タンパー性や課金その他の機能を正しく放送局の定める仕様に従って実装していることを放送局側の放送管理システム８との間の通信によって証明することが望ましい。この場合、例えば、受信装置１が自装置の識別番号を放送管理システム８に対して証明する。この証明を通信によらず例えば監視員による査察などの方法で行うことは人件費の点から非現実的であることは言うまでもない。

【００４９】この場合に、証明に用いる受信装置１内部に記憶されている装置識別子も耐タンパー性などにより外部からのアクセスを禁止するようにする。なお、この受信装置１が放送局側に正当な装置識別子を持つことを証明する手続きには、データ自体の受け渡しをせずにそのデータの内容の認証を可能とするゼロ知識証明方式を用いるのが望ましい。ゼロ知識証明方式については、例えば、Fiat Shamirのゼロ知識証明法が「Fiat, A., Shamir, A. : “How to prove yourself : practical aolution to identification andsignature problems”, Proc. of CRYPTO86, Springer－Verlag, Berlin, 1987」に開示されている。

【００５０】また、放送局側に対して、受信装置１がある装置識別子ｐを持つことを証明するとき、ゼロ知識証明方式を用いる代わりに、識別子ｐを暗号化して送る方法を用いることもできる。その手順の一例を次に示す。

【００５１】相手の放送局は秘密鍵ｅと公開鍵ｆを持ち、受信装置１は公開鍵ｆを知っている。受信装置１は、公開鍵ｆによって識別子ｐを暗号化して放送局に鍵を送信する。放送局は公開鍵ｆに対応する秘密鍵ｅによって直接識別子ｐを得ることができる。一方、第３者は秘密鍵ｅを知らないので、たとえ公開鍵ｆによって暗号化された識別子ｐのデータを傍受できたとしても、傍受したデータから直接識別子ｐを得ることはできない。また、公開鍵ｆと傍受したデータからこれらに対応する識別子ｐを得るには非常に大きな計算量が必要になり、事実上、識別子ｐを得ることは不可能とみなすことができる。

【００５２】このような技術は既に多数存在するが、その１つとしてＲＳＡ暗号がよく知られている。このＲＳＡ暗号については、例えば、「R. L. Rivest, A. Shamir, and L. M. Adelman, “A method for obtaining digital signatures andpublic－key cryptosystems”, C

ommunications of ACM、２１（２）、１９７８」に開示されている。

【００５３】ただし、悪意の第３者が放送局を詐称している場合、この方法では識別子の秘密が漏れてしまう可能性があるため、事前に受信装置に対して放送局が正しいものであることを証明する逆の認証手順が必要になる。

【００５４】なお、他の方法には、Ｄｉｆｆｙ－Ｈｅｌｌｍａｎの鍵共有プロトコルを利用するものなどが考えられる。以下では、これまでに説明したような基本構成を有するいくつかの受信装置について詳しく説明する。

【００５５】図３に、本実施形態に係る受信装置１の構成の一例を示す。ここでは、放送される放送信号は、圧縮処理され暗号化されているものとする。

【００５６】１４－１～１４－ｎはそれぞれ入力ライン１～ｎを表す。これらは地上波放送（ＶＨＦ／ＵＨＦ）、衛生放送、ケーブルＴＶなどの入力にそれぞれ対応する。この受信装置１は、同調・復調回路２１－１～２１－ｎ、復号化部２２、伸張符号化部２３、識別信号付加部２４、圧縮部２５、出力回路２６、復号化鍵・加入者情報管理装置２７、装置識別子２８を備えている。

【００５７】同調・復調回路２１－１～２１－ｎは、それぞれ独自の周波数／変調方式で変調された入力に対応する同調・復調回路であり、ここで入力信号はデジタル信号に変換される。なお、どのような方式に対応した同調・復調回路を何種類備えるかは任意である。

【００５８】復号化部２２は、同調・復調により得られた、暗号化されたデジタル信号を復号する。これによって圧縮符号化された信号が得られる。なお、図３においては復号化機能は単一のものとして扱われているが、複数の方式が存在し、その方式毎に機能ブロックを分割しても良い。

【００５９】伸張符号化部２３は、復号により得られた、圧縮符号化された信号に対し、伸張符号化を施して、もとの信号を得る。識別信号付加部２４は、復号化と伸張により得られた信号に、識別信号を付加する。

【００６０】圧縮部２５は、上記の識別信号を付加された信号を、出力インタフェースの符号化形式で圧縮符号化する。出力回路２６は、この圧縮符号化された信号を放送ライン１５へ出力する。

【００６１】そして、この出力は、加入者の再生装置に伝えられ、再生が行われる。なお、ここでは出力インタフェースはデジタル変調を仮定している。もしアナログ出力を行う場合には圧縮符号化を行う必要はなく、圧縮部２５は省かれる。

【００６２】復号化鍵・加入者情報管理装置２７は、通信回線１６を通じて放送管理システム８に自装置が正しい装置識別子２８を持つことを証明し、復号化鍵および番組に付加する識別情報を取得する手続きを行う。復号化鍵は復号化部２２に、識別情報は識別情報付加部２４に知らされる。

【００６３】本構成において、耐タンパー性が必要とされるのは、ハッチングされた部分２９によって示した復号化部２２、伸張符号化部２３、識別情報付加部２４、復号化鍵・加入者情報管理部２７、装置識別子２８とそれらのブロック間の接続を含む部分である。もちろんそれ以外の部分を耐タンパー性をも持つ形で実装しても構わない。

【００６４】ここで識別信号の付加前に一度伸張符号化を行う理由の１つは入力と出力で圧縮の形式が異なる場合があるためである。例えば放送局側はＭＰＥＧ２符号化を使用し、出力側はＤＶフォーマットを使用している場合がこれにあたる。

【００６５】もう１つの理由は識別情報の付加の方式において原信号の周波数スペクトルなどの情報を利用する技術（例えば、“Ｄｉｇｉｔａｌ Ｗａｔｅｒｍａｒｋｓ ｆｏｒ Ａｕｄｉｏ Ｓｉｇｎａｌｓ”，Ｌ．Ｂｏｎｕｅｙ 他，Ｐｒｏｃｅｅｄｉｎｇｓ ｏｆ Ｉｎｔｅｒｎａｔｉｏｎａｌ Ｃｏｎｆｅｒｅｎｃｅ ｏｎｍｕｌｔｉｍｅｄｉａ ｃｏｍｐｕｔｉｎｇ ａｎｄ ｓｙｓｔｅｍｓ，ＩＥＥ，１９９６）を利用する場合、これらの圧縮符号化された信号をそのままに識別情報を付加することが画質の低下などの理由によって困難な場合があるためである。

【００６６】入力と出力の符号化形式が同一であり、上記の画質の低下などの問題を持たない識別信号の付加形式が利用可能であるという条件においては、伸張符号化および圧縮符号化を行うことなく圧縮符号化された原信号に直接識別信号を付加する構成をとることによってシステムの規模とコストを低減することが可能である。

【００６７】次に、図４に、本実施形態に係る受信装置１の構成の他の例を示す。ここでは、放送される信号は、圧縮処理され暗号化されているものとする。本構成例は、識別信号を付加した後、圧縮符号化を行わない場合に対応するものであり、図３の圧縮符号化部２５を持たないこと以外は図３の場合と同様である。出力はデジタル変調でもＮＴＳＣのようなアナログ変調のどちらでも良い。本構成において耐タンパー性が必要とされる部分をハッチングされた領域２９によって示す。

【００６８】次に、図５に、本実施形態に係る受信装置１の構成の他の例を示す。ここでは、放送される信号は、圧縮処理され暗号化されているものとする。本構成例は、伸張符号化を行うことなく識別信号を付加して出力する場合に対応するものであり、図３の構成から伸張符号化部２３と圧縮符号化部２５を省いたものである。ただし、この場合、識別情報付加部２４は、画質の低下なしに、圧縮符号化された信号にそのまま識別信号を付加可能な方式を用いるものとする。本構成において耐タンパー性が必要とされる部分を領域２９によって示す。

【００６９】以下では、これまで説明してきた受信装置

により番組を視聴する際の手順について説明する。この手順の一例を図６に示す。

【００７０】番組の視聴は、ユーザによる番組視聴要求によって始まる（ステップＳ３１）。番組視聴要求は、ユーザの操作によって受信装置１に付属するリモコン装置もしくはタイマ予約装置から、または接続されている再生／記録装置もしくは通信インタフェース１６から入力される。通信インタフェース１６を用いる場合は、加入者以外の第３者によるアクセスの可能性があるため、暗号あるいはパスワードを用いて認証するなど適切なセキュリティ対策を行うことが望ましい。

【００７１】番組視聴要求を受けると、受信装置１は、自装置が正当な装置であることを証明する手続きを放送局側の放送管理装置８との間で行う（ステップＳ３２）。その証明が行われた後に放送管理装置８に番組を要求し（ステップＳ３３）、対応する復号鍵を得る。番組の要求には、既にあるチャネルにおいて放送されている場合にはチャネル情報を、ＶＯＤのようにユーザの要求によって開始される放送サービスではその番組の情報を用いる。受信装置１と放送管理装置８との間で行うデータの受け渡しについては、復号鍵の配送のみならず、その他の手続きについても個人のプライバシーを守るために適切な方法により暗号化され、第３者がその内容を知ることのできないようにすることが望ましい。

【００７２】復号鍵を得た受信装置１は、放送信号に付加する識別信号に含ませる情報として、識別番号の他にこれに付加する情報について放送局側からの指示を受ける処理を実行する（ステップＳ３４）。識別信号には、例えば、放送局識別情報、加入者装置識別情報、加入者識別情報（単一の加入者装置において複数の視聴者が存在する場合）、番組識別情報、所定の基準時からの絶対時刻、および番組開始からの経過時間などの情報が含まれる。不正コピーの流通を防ぐ面からは加入者情報（加入者装置情報）や番組識別情報は全世界で一意となるようにしておくことが望ましい。放送局識別情報が全世界で一意であれば、それぞれの放送局の加入者装置で識別情報を一意に設定しておけばこれが実現できる。

【００７３】さらに、これらの情報が確かにその情報を放送した放送局のものであることを示すために、これらの情報はその放送局の持つ秘密鍵で暗号化され、それに対応する公開暗号鍵で復号化することによって正しく読むことのできる認証子を付加しておくことが望ましい。これを行わない場合、ある番組の原信号を持つ悪意の第３者は、任意の放送局の識別情報を前記信号に付加することにより、あたかもその番組が当該放送局によって放送されたと偽ることが可能となるおそれがあるからである。

【００７４】次に、受信装置１は、再生可能な信号を再生機器に送出する（ステップＳ３５）。なお、放送信号の復号鍵は、鍵情報の漏洩による被害を防ぐためにある期間毎に変更される。例えば、番組単位、もしくは一定時間単位である。ただし、この間隔が長くなれば鍵情報が漏洩する可能性が高くなり、短くなれば鍵情報の配送のオーバーヘッドが大きくなることはいうまでもない。

【００７５】また、鍵情報の変更と、放送の視聴による課金はかならずしも対応していなくとも良い。例えば鍵情報の変更が１日に１回の場合であっても、放送の視聴単位は１日よりも小さな時間単位によって管理されても良い。この場合、受信装置１は加入者が視聴を望まない時間には、鍵情報をもっていても放送の復号化を行わず、その時間は課金を行わない。この場合、ステップＳ３５で、再生可能な信号を再生機器に送出する処理の開始とともに課金を開始する。一方、鍵情報の変更と、放送の視聴による課金を対応させる場合、ステップＳ３４で課金を開始する。その他、課金の仕方には種々の方法が適用可能である。

【００７６】また、番組の視聴時刻および番組開始からの経過時間については、放送管理システム８からそれらの情報を受けずに受信装置１がそれらを管理するための時計を持つことによって通信回線の使用を低減することができる。視聴時刻および番組開始からの経過時間を示す情報は放送に付随する信号に基づいても良い。

【００７７】以上では、放送局が放送によって配布する著作物に識別信号を付加する説明をしてきた。著作権者から放送局への著作物配布にあたっても、当然このような識別信号が付加されることが考えられる。著作権者から放送局への複製の段階と、放送局からエンドユーザである利用者への複製の段階でそれぞれ別の識別信号が付加されるものである。このように複数回にわたって識別情報が付加される場合においても、識別情報の読み取りで互いの識別性を損なったり、著作物の品質を低下させることが防がれなければならない。その方法について以下に説明する。

【００７８】図７に識別信号付加方式の変更を含む場合の手順を示す。図６の手順との相違は、放送局からの情報を取得するステップＳ４４において放送信号に付加されている識別情報の形式を取得していること、およびステップＳ４５において先に取得した識別情報の形式に基づいて受信装置１において付加する識別情報の形式を変更することである。

【００７９】例えば著作物が音声であり、識別信号は著作物に関する情報列をＭ系列に基づく符号語によって変調して可聴周波数帯域内にスペクトル的に拡散した信号であって、原信号と識別信号の線形和を取ることによって信号の付加を行っている場合を考える。識別信号は、原信号によって人間の聴覚特性的に抑圧されて聞き取ることのできない強度で付加する。人間の聴覚特性的にはこのような信号強度のしきい値が存在することが知られている。

【００８０】識別信号の解読は、原信号をＳ、識別信号

を付加された信号をＳ´とすると、両者の差Ｓ´－Ｓを復調することによって行うことができる。すなわち、原信号を用いることにより、受信装置１の出力信号Ｓ´から識別信号を再生することができる。

【００８１】ここで、放送局から送出する時点において付加されている識別信号を識別信号１、受信装置において付加する識別信号を識別信号２とする。複数回にわたって識別信号を付加する場合においても識別信号１と識別信号２の信号の和のパワースペクトラムが原信号に対して聴覚特性的に抑圧されるしきい値以下であれば、信号の付加が著作物の品質を損なうことはない。

【００８２】識別信号の再生は、２つの信号の和信号から復調することになるが、識別信号１と識別信号２が互いに直交する符号を使用している場合は互いに干渉しないため問題はない。これは符号語の周期が同一である場合、Ｍ系列と呼ばれる符号の組を用いることにより実現できる。また、同じ符号語を使用している場合にも変調の周期をビットと呼ばれるある相対的な期間以上ずらすことにより、複数の識別子が互いに干渉することなく再生できることが知られている（“ＳｐｒｅａｄＳｐｅｃｔｒｕｍ　Ｓｙｄｔｅｍｓ”，Ｒ．Ｄｉｘｏｎ，１９７６）。

【００８３】したがって、予め直交する符号後の組を定めておき、ステップＳ４４において、放送局は著作物に付加されている識別情報の符号語を受信装置１に知らせることによって、受信装置１はそれに合致しない符号の識別信号付加手段を選択することができる。識別情報の符号語を直接送信するのではなく、符号語の組の中で符号語を識別するための識別子を予め定めておき、符号語に対応する識別子を送信しても良い。

【００８４】また、受信装置１が１種類の符号に基づく信号付加手段しか持たない場合には、識別信号１の符号的な位相関係を示す情報を受信装置が得ることにより、受信装置は適切な期間だけ識別信号の位相をずらすことによって識別信号１と識別信号２の干渉を防ぐことができる。

【００８５】なお、上記では、信号を放送局から送出する時点において付加されている識別子は１種類のみとしたが、これは流通の複数段階に対応して複数あっても良い。本発明は、上述した実施の形態に限定されるものではなく、その技術的範囲において種々変形して実施することができる。

【００８６】

【発明の効果】本発明によれば、放送系やビデオオンデマンドのように同一の著作物が複数のユーザに配布される、加入者を限定した放送システムにおいて、加入者側に設置される受信装置において、自装置から出力される信号に加入者（受信者）を特定する信号を付加するようにすることで、加入者毎に別々の識別情報を付加することができる。

【００８７】これによって、不法に著作物の複製が頒布・販売されるのを未然に防止するとともに、万一、放送された著作物が複製され流通されたとしても、その出所を特定することができる。

【図面の簡単な説明】

【図１】本発明の一実施形態に係るシステムの構成を示す図

【図２】同実施形態に係る受信装置の基本構成を示す図

【図３】同実施形態に係る受信装置の一構成例を示す図

【図４】同実施形態に係る受信装置の他の構成例を示す図

【図５】同実施形態に係る受信装置のさらに他の構成例を示す図

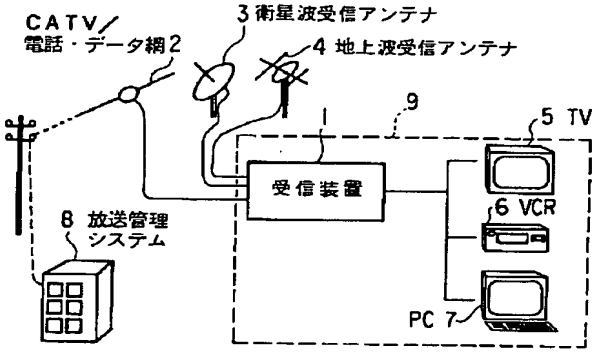
【図６】同実施形態に係る番組視聴手順の一例を示すフローチャート

【図７】同実施形態に係る番組視聴手順の他の例を示すフローチャート

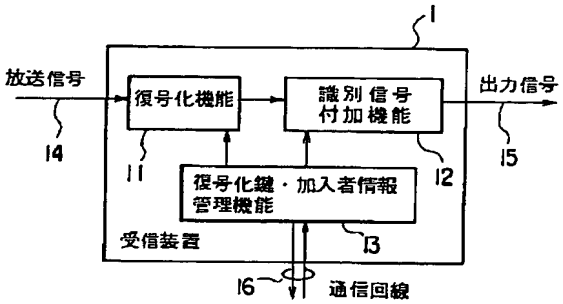
【符号の説明】

１…受信装置
２…外部のネットワーク
３…衛星放送受信アンテナ
４…地上波放送受信アンテナ
５…ＴＶ
６…ＶＴＲ
７…パーソナルコンピュータ
８…放送管理システム
９…加入者宅内システム
１１，２２…復号化部
１２，２４…識別信号付加部
１３，２７…復号化鍵・加入者情報管理部
１４，１４－１～１４－ｎ…入力ライン
１５…出力ライン
１６…通信回線
２１－１～２１－ｎ…同調・復調回路
２３…伸張符号化部
２５…圧縮部
２６…出力回路
２８…装置識別子

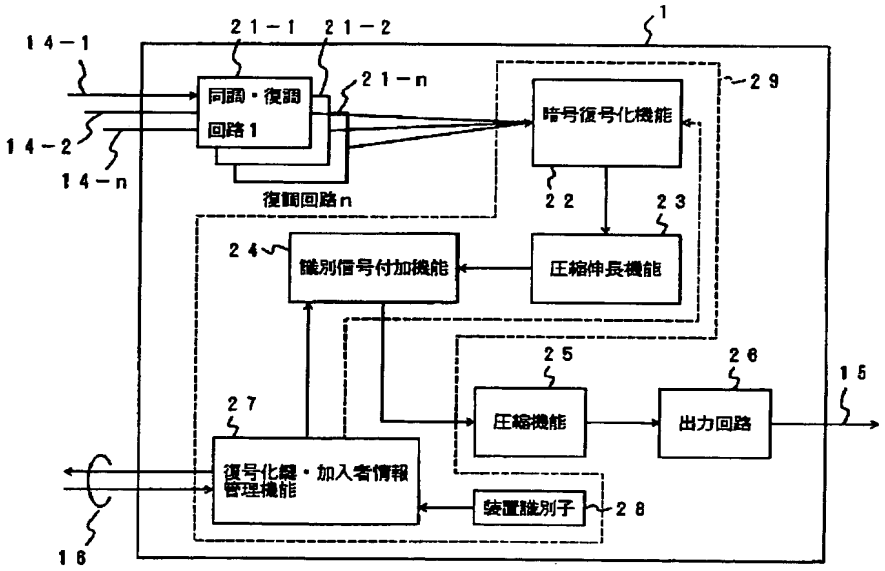
【図１】


CATV
電話・データ網2
3 衛星波受信アンテナ
4 地上波受信アンテナ
9
5 TV
1
受信装置
6 VCR
8 放送管理
システム
PC 7

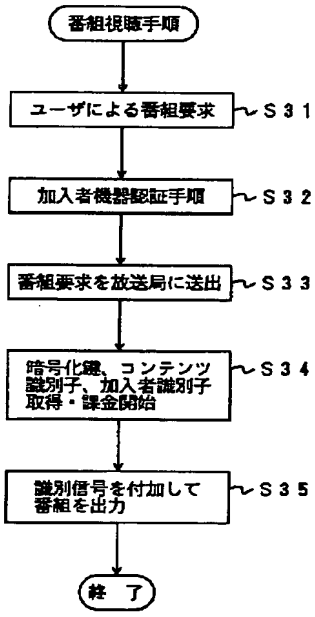
【図２】


1
放送信号
復号化機能
識別信号
付加機能
出力信号
14
11
12
15
復号化鍵・加入者情報
管理機能
受信装置
13
16
通信回線

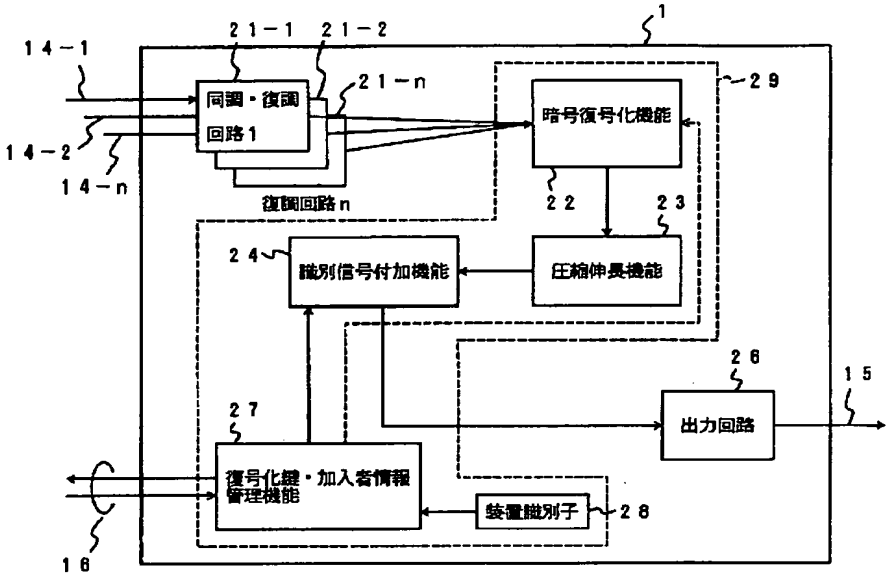
【図３】


14－1
14－2
14－n
21－1
21－2
21－n
同調・復調
回路1
復調回路n
1
29
暗号復号化機能
22
23
24
識別信号付加機能
圧縮伸長機能
25
26
15
27
圧縮機能
出力回路
復号化鍵・加入者情報
管理機能
装置識別子
28
16

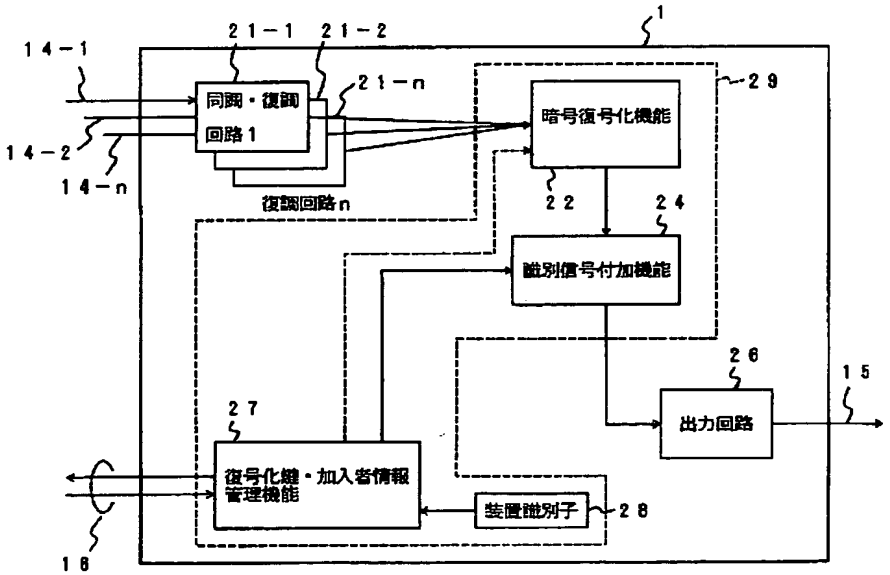
【図６】


番組視聴手順
ユーザによる番組要求
S31
加入者機器認証手順
S32
番組要求を放送局に送出
S33
暗号化鍵、コンテンツ
識別子、加入者識別子
取得・課金開始
S34
識別信号を付加して
番組を出力
S35
終了

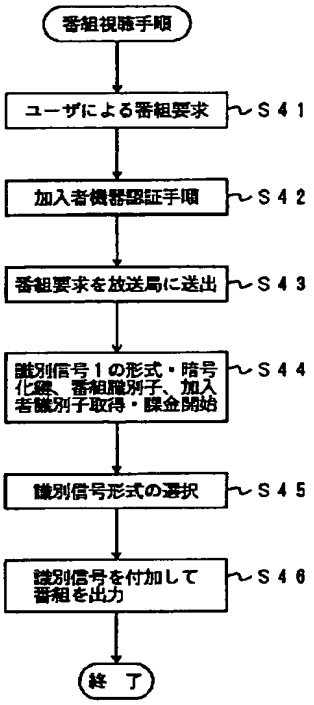
【図４】


1
14－1
14－2
14－n
21－1
21－2
21－n
同調・復調
回路1
復調回路n
暗号復号化機能
29
22
23
圧縮伸長機能
24
識別信号付加機能
26
出力回路
15
27
復号化鍵・加入者情報
管理機能
装置識別子
28
16

【図５】


1
14－1
14－2
14－n
21－1
21－2
21－n
同調・復調
回路1
復調回路n
暗号復号化機能
29
22
24
識別信号付加機能
26
出力回路
15
27
復号化鍵・加入者情報
管理機能
装置識別子
28
16

【図７】


番組視聴手順
ユーザによる番組要求
S41
加入者機器認証手順
S42
番組要求を放送局に送出
S43
識別信号１の形式・暗号化鍵、番組識別子、加入者識別子取得・課金開始
S44
識別信号形式の選択
S45
識別信号を付加して番組を出力
S46
終了